UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | ) | |
| | ) | |
| v. | ) | No.: 16-cr-10305-NMG |
| | ) | |
| MARTIN GOTTESFELD, | ) | |
| | ) | |
| Defendant. | ) | |

GOVERNMENT'S OPPOSITION
TO DEFENDANT GOTTESFELD'S SUPPLEMENTAL
MOTIONS TO SUPPRESS EVIDENCE

The United States of America, by Assistant United States Attorneys David J. D'Addio and Seth B. Kosto, hereby opposes Defendant Martin Gottesfeld's Supplemental Motion to Suppress (Dkt. No. 128) and his Second Supplemental Motion to Suppress Evidence (Dkt. No. 166).

## I. INTRODUCTION

For the third time in nine months, Gottesfeld seeks to suppress evidence obtained during the October 1, 2014 execution of a search warrant at his Somerville apartment. In August 2017, Gottesfeld's then counsel, Jane Peachy, Esq., filed his first effort, (Dkt. No. 78), which focused on: (1) whether the use a pen register and trap and trace ("PRTT") device to collect Internet Protocol ("IP") addresses reflecting Gottesfeld's internet traffic violated the Fourth Amendment, and (2) whether the warrant was sufficiently particular. *Id*. The government opposed the motion on October 11, 2017, and the Defendant filed a reply on October 20, 2017, (Dkt. Nos. 84, 89).

In March 2018, successor counsel Raymond Gillespie, Esq., filed the next installment in Gottesfeld's suppression trilogy. (Dkt. No. 128). In that motion, Gottesfeld argued that: (1) "port numbers" used to route internet traffic constitute the "content" of Gottesfeld's

communications, and therefore the government was prohibited from obtaining those port numbers through a PRTT device; (2) the affidavit filed in support of the search warrant failed to establish probable cause to search Gottesfeld's apartment; and (3) "the only explanation for [the search warrant's] issuance appears to be an unacknowledged bias and conflict of interest on the part of the issuing magistrate judge," (Dkt. No. 128 at 2).

Gottesfeld's latest counsel, David Grimaldi, Esq., filed the final installment on May 4, 2018. (Dkt. No. 166). In this motion, Gottesfeld adopted all of his prior arguments and incorporated each of his prior motions and all their attachments by reference. (Dkt. No. 166 at 1). The third motion primarily adds allegations of judicial misconduct by Magistrate Judge Marianne B. Bowler, who issued the warrant to search Gottesfeld's apartment. Specifically, Gottesfeld argues: (1) Judge Bowler's alleged involvement with The Boston Foundation, a charity that has supported Boston Children's Hospital and Wayside Youth and Family Services; and (2) the work of Judge Bowler's husband for the Harvard Medical School ("HMS") and the Brigham and Women's Hospital ("BWH") each created both an actual conflict of interest and the appearance of a conflict of interest that required Judge Bowler to recuse herself from considering the search warrant application. Gottesfeld further argues that the warrant was defective on its face because of a typographical error on the application cover sheet, and that the affidavit in support of the warrant failed to establish probable cause. Coupled with the alleged conflicts of interest, these defects, Gottesfeld argues, preclude good-faith reliance on the warrant.

## II. SUMMARY OF ARGUMENT

Each of Gottesfeld's arguments lack a factual basis, a legal basis, or both. With respect to recusal, Judge Bowler had no formal or informal relationship with The Boston Foundation at the time she authorized the search of Gottesfeld's apartment. Gottesfeld's assertion to the

contrary is false and cannot support an argument for recusal. The fact that Judge Bowler's husband is employed by a medical school and a hospital that were not the target of attack bring investigation similarly provides no grounds for recusal.

The government's collection of port data for Gottesfeld's internet traffic was both proper and entirely unrelated to the evidence he seeks to suppress. First, port data constitutes nothing more than "dialing, signaling, addressing, or routing" information within the meaning of the statute authorizing its collection, 18 U.S.C. § 3121-27 (the "Pen/Trap Act"). The collection of port data raises even fewer Fourth Amendment concerns than the collection of IP address data, which every court to consider the question has found to be within the scope of the Pen/Trap Act. Port data, like IP addresses, is typically unencrypted and is both available to and sometimes monitored by internet service providers.

The search warrant affidavit in any event did not refer to port data at all; it referred only to domain names associated with the IP addresses for websites Gottesfeld visited. Thus, even if the court were to conclude that the Pen/Trap Act did not authorize the collection of port data (or that it did so in violation of the Fourth Amendment), Gottesfeld makes no claim that the use of that port data led to the acquisition of any evidence he seeks to suppress. The Court therefore need not determine whether the collection of port data was proper under the Pen/Trap Act or the Fourth Amendment.

In short, there are no grounds to suppress the evidence obtained from the October 1, 2014 search. To the extent the Court finds any error at all, suppression would not be an appropriate remedy, as the agents relied in good faith on a court order issued pursuant to a presumptively valid statute, case law supporting the collection of IP addresses, and a facially valid search warrant.

## III. ARGUMENT

### A. Legal Principles Concerning Recusal

A magistrate judge issuing a search warrant must satisfy two constitutional requirements: the judge "must be neutral and detached, and . . . must be capable of determining whether probable cause exists for the requested arrest or search." *Shadwick v. City of Tampa*, 407 U.S. 345, 350 (1972). Courts have identified two principal categories of cases in which magistrates have failed to meet this constitutional standard: (1) when the magistrate had a direct pecuniary interest in issuing the warrant, *e.g.*, *Connally v. Georgia*, 429 U.S. 245, 251 (1977) (unsalaried justice of the peace not neutral and detached because he received $5 per warrant issued), and (2) when the magistrate played a role in the law enforcement investigation, *e.g.*, *Coolidge v. New Hampshire*, 403 U.S. 443, 450 (1971) (state attorney general not neutral and detached where he oversaw the investigation and prosecuted the case at trial). *See generally United States v. Harris*, 566 F.3d 422, 433 (5th Cir. 2009) (discussing the two categories of cases); *United States v. Bowers*, 828 F.2d 1169, 1174–75 (6th Cir. 1987) (same).

Separately, 28 U.S.C. § 455 also governs judicial recusals. Section 455(a) is designed to avoid the *appearance* of partiality and requires recusal whenever the judge's "impartiality might reasonably be questioned." Section 455(b), in contrast, requires recusal when *actual* conflicts of interest arise, including when the judge:

> (4) . . . knows that he, individually or as a fiduciary, or his spouse . . . has a financial interest in the subject matter in controversy or in a party to the proceeding, or has any interest that could be substantially affected by the outcome of the proceeding; [or]

> (5) He or his spouse . . . :
> (i) Is a party to the proceeding, or an officer, director, or trustee of a party; . . . [or]
> (iii) Is known by the judge to have an interest that could be substantially affected by the outcome of the proceeding[.]

28 U.S.C. § 455(b).

By addressing the appearance of conflicts, section 455(a) "vindicates the interests of the judicial system as a whole" and "preserve[s] public confidence in the courts." *United States v. Murphy*, 768 F.2d 1518, 1539-40 (7th Cir. 1985). It is not designed to protect individual rights, however, because the mere "appearance of impropriety does not undercut personal rights." *Id*. at 1540. Indeed, recusal under § 455(a) typically applies only prospectively and does not require orders issued before recusal to be vacated. *See, e.g.*, *El Fenix de P.R. v. M/Y Johanny*, 36 F.3d 136, 141-42 (1st Cir. 1994) (error to setting aside final judgment that was entered before recusal under § 455(a)).

The Fourth Amendment's neutrality requirement, in contrast, is a personal right that is violated when a judge faces a conflict of interest so significant that the judge is no longer "neutral and detached." This distinction led the Fifth Circuit to conclude that section 455(a) does not provide the appropriate standard in assessing the neutrality of a magistrate who issues a warrant. *See Harris*, 566 F.3d at 434; *People v. Gallegos*, 251 P.3d 1056, 1063 (Colo. 2011) (holding that "statutory disqualification analysis is not the relevant inquiry" in the Fourth Amendment context); *see also United States v. Couch*, 896 F.2d 78, 81 (5th Cir. 1990) ("As this and several other circuits have recognized, section 455 establishes a statutory disqualification standard more demanding than that required by the Due Process Clause."). Gottesfeld's emphasis on the appearance of impropriety is therefore misplaced. He must demonstrate an

*actual* conflict of interest that deprived him of his Fourth Amendment rights—not merely the appearance of one.

Although determining the correct legal framework is important, it ultimately does not affect the outcome here, as Gottesfeld has failed to show either the appearance of any bias or its actual manifestation on the part of Judge Bowler.

B. Magistrate Judge Bowler Had No Relationship with The Boston Foundation When She Issued the Warrant.

Gottesfeld has argued in successive motions to suppress (and in other filings) that Judge Bowler's involvement with The Boston Foundation ("TBF") created a conflict of interest that disqualified her from issuing the warrant to search Gottesfeld's apartment. TBF is a philanthropic organization that, among other things, supports Boston area institutions and community programs through grants. Gottesfeld claims that Judge Bowler was serving as a "director emeritus" of TBF in September 2014 when she issued the warrant. (Dkt. No. 166 at 14). He then claims that TBF made grants to both the Boston Children's Hospital and Wayside Youth and Family Services (victims of Gottesfeld's DDOS attacks), *id.* at 12; that Judge Bowler either was aware of these grants or should have been aware of them when she issued the warrant, *id.* at 12-13; that Judge Bowler owed a legal fiduciary duty to TBF, including a duty of care and a duty of loyalty, when she issued the warrant, *id.* at 14; and that some of the money donated by TBF to Boston Children's Hospital and Wayside Youth and Family Service would have been used cover to losses incurred from the DDOS attacks, *id*. at 14.

This argument fails at the outset because it is built on a false premise. Judge Bowler had no relationship with TBF when she issued the warrant—she was neither a board member nor a director emeritus; she had not advised or counseled TBF, formally or informally, on any matters

since 2005. In fact, the position Gottesfeld claims Judge Bowler held in September 2014—Director Emeritus—did not exist when she issued the warrant.

As set forth in the affidavit of TBF's Corporate Secretary, Timothy Gassert, TBF amended its bylaws on October 16, 2014—weeks after Judge Bowler issued the warrant—to create the status of "Director Emeritus" in order "to recognize the service of directors who had served two, complete five-year terms on the Board of Directors." (Exhibit A hereto at ¶ 3). Judge Bowler was a TBF board member from 1995 until 2005. *Id*. at ¶ 2. From that point forward, however, Judge Bowler "has not held a position with the Boston Foundation that would allow her to exercise any corporate authority over Boston Foundation matters, including the awarding of grants or other philanthropic activities; nor has her advice or counsel been sought or received on any such matters." *Id*. "Director Emeritus" is an honorific title: "As a result of having served two, complete, five year terms, [Judge] Bowler has been recognized as a director emerita of the Boston Foundation. [Judge] Bowler has not been invited by a chair of the Board of Director to serve as an *ex officio* member of any Board committee nor to serve in any other official capacity, and has not exercised any authority on behalf of the Boston Foundation, since leaving the Board in 2005." *Id*. at ¶ 4.

Defendant's claim that Judge Bowler had any ongoing relationship with TBF, let alone one that would violate a constitutional standard of neutrality, is a fiction, not a ground for suppression.[1] To the extent that Gottesfeld argues that Judge Bowler's membership on the TBF

[1] Because Judge Bowler played no role in TBF matters, the government does not address the many secondary problems with Gottesfeld's argument. The government notes only that the relationship between the entities is not as significant as Gottesfeld suggests. Donations to Children's Hospital appear to account for approximately 0.19% of grants made by TBF and 0.06% of the grants received by Children's Hospital in the year for which Gottesfeld obtained documentation.

board of directors some 9 years before she signed the warrant was grounds for recusal, he fares no better. Courts have consistently rejected as grounds for recusal connections to matters and defendants that are far less attenuated than those described here. *See, e.g.*, *United States v. Bowling*, 619 F.3d 1175, 1186 (10th Cir. 2010) (magistrate was neutral and detached despite having previously represented a bank in an adverse legal proceeding against the defendant); *Harris*, 566 F.3d 422, 433-34 (5th Cir. 2009) (magistrate was neutral and detached despite having previously represented defendant in unrelated matter); *United States v. Outler*, 659 F.2d 1306, 1312 (5th Cir.1981) (magistrate was neutral and detached despite having prosecuted defendant three years earlier in unrelated case). The government is aware of no case in which recusal was required because of a nearly decade-old professional relationship with an organization that provided grants to a victim of a crime. *Cf. Roth v. City of Canton*, 2017 WL 528348, *2-3 (N.D. Ohio Feb. 8, 2017) (judge refused to recuse based on her service on a non-party charity's board of directors where the judge had not been active with the charity's board for several years and had no "ongoing relationship with the Society's leadership and management"). As a former judge in this District noted, "all judges had full professional lives—as prosecutors, as corporate lawyers, as civil rights lawyers—before they were appointed to the bench." *Rosenberg v. Merrill Lynch, Inc.*, 976 F. Supp. 84, 85–86 (D. Mass. 1997) (Gertner, J.). Gottesfeld's claim that Judge Bowler's relationship with TBF gave rise to a conflict—whether actual or in appearance only—is entirely without merit.

C. Judge Bowler's Husband Had No Financial Interest in the Matter That Would Have Required Her Recusal.

Defendant correctly notes that Judge Bowler is married to Marc A. Pfeffer, M.D., Ph.D., who is the Dzau Professor of Medicine at Harvard Medical School ("HMS") and a senior cardiologist at the Brigham and Women's Hospital ("BWH"). (Dkt. No. 166 at 3). While

Gottesfeld notes that Children's Hospital and BWH are "affiliates" of HMS, he erroneously concludes from this that "both of Dr. Pfeffer's employers, HMS and BWH, are affiliates of alleged 'organizational victim' BCH."[2]

By lumping together HMS and each of its "affiliated" entities, Gottesfeld suggests Dr. Pfeffer's employment at BWH and HMS gave him a financial interest in the outcome of the application for a search warrant. (Dkt. No. 166 at 7-8). Gottesfeld alleges that because of this purported financial interest, Judge Bowler "violated § 455(b)(4) and (b)(5)(iii)" by issuing the warrant. *Id.* at 7.

As noted, section 455(b)(4) [3] mandates recusal where a judge's "spouse . . . has a financial interest in the subject matter in controversy or in a party to the proceeding, or any other interest that could be substantially affected by the outcome of the proceeding." 28 U.S.C. § 455(b)(4). A victim of a crime, however, is not a "party to the proceeding" under § 455(b)(4). *United States v. Rogers*, 119 F.3d 1377, 1384 (9th Cir. 1997). Similarly, a financial interest in a corporate victim "cannot be deemed a financial interest in the subject matter in controversy" under § 455(b)(4). *Rogers*, 119 F.3d at 1384; *accord United States v. Nobel*, 696 F.2d 231, 234

[2] Defendant frequently attempts to merge together distinct medical entities in this case by calling them "affiliates." The affiliation between these entities has nothing to do with "shareholdings or other means of control"; nor is any entity "a subsidiary, parent, or sibling corporation." *Black's Law Dictionary* (10th ed. 2014) (defining "affiliate"). Instead, the relationship between HMS and area hospitals (including Children's Hospital and BWH) relates to training medical students and residents. "Unlike many medical schools, HMS does not own or operate hospitals, relying instead on agreements with 16 clinical affiliates and research institutes, vital partners that provide patient care and clinical training." *See* https://hms.harvard.edu/about-hms/hms-affiliates (accessed May 17, 2018). HMS, Children's Hospital, and BWH are parts of distinct, independent entities with their own leadership and organizational structures.

[3] Sections 455(b)(4) and 455(b)(5)(iii) are redundant insofar as they apply to a judge's spouse, *see In re SunEdison, Inc.*, 2016 WL 2849482, at *2 (Bankr. S.D.N.Y. 2016), so the government treats them together.

(3d Cir. 1982). Therefore, even if Dr. Pfeffer had a *direct* financial interest in Children's Hospital (which he does not), he would not have an interest in a "party to the proceeding" or the "subject matter in controversy" under § 455(b)(4). If recusal was required under § 455(b)(4), it could thus only be because Dr. Pfeffer had some other "interest that could be substantially affected by the outcome of the proceeding." 28 U.S.C. § 455(b)(4).

Gottesfeld offers no coherent explanation of how Dr. Pfeffer could have a financial interest that "could be substantially affected" in the outcome of an *application for a search warrant* (as opposed to, for example, civil litigation involving an employer). Dr. Pfeffer is an adult cardiologist affiliated with the Brigham and Women's Hospital. He does not admit patients to Children's Hospital, take care of them there, or instruct the medical students and residents who are learning to take care of the pediatric patients admitted to Children's Hospital. *See* http://profiles.ehs.state.ma.us/Profiles/Pages/PhysicianProfile.aspx?PhysicianID=29959 (Dr. Pfeffer's Board of Registration of Medicine listing) (accessed May 18, 2018).

Against this reality, Gottesfeld cobbles together possible financial interests, none of which, either alone or collectively, required recusal. As a point of comparison, there is ample authority holding that a judge need not recuse herself from a case where one party is represented by a law firm that employs the judge's family member as an associate. *See United States ex rel Weinberger v. Equifax, Inc.*, 557 F.2d 456, 463 (5th Cir. 1977); Leslie W. Abramson, *The Judge's Relative is Affiliated with Counsel of Record: The Ethical Dilemma*, 32 Hofstra L. Rev, 1181, 1197 n.65 (2004) (collecting cases). Just as an associate's salary interest in his firm's victory or defeat "is too remote to fall under this 'financial interest' prohibition," *Weinberger*, 557 F.2d at 463, Dr. Pfeffer's salary interest is too remote in this case to create even an appearance of bias on the part of Judge Bowler.

D. Judge Bowler's Husband Had No Non-Financial Interest in the Matter that Would Have Required Her Recusal.

Gottesfeld also suggests that Dr. Pfeffer had non-financial interests in the outcome of the application for a search warrant. (Dkt. No. 166 at 4-5, 8). Specifically, he argues that Dr. Pfeffer is associated with BWH's "Division of Medical *Communications*," *id*. at 4 (emphasis added); the DDOS attack affected a computer network on which BWH "*communicates*," *id.* (emphasis added); and therefore, Dr. Pfeffer's work in the Division of Medical *Communications* was affected, *id.* (emphasis added). Defendant is playing games with words, not mounting a serious argument. As Gottesfeld is no doubt aware, the Division of Medical Communication focuses on physician communications skills, not computer networks. The web page for BWH's Division of Medical Communications states:

> Excellent physician communication skills (physician-to-patient and patient-to physician) have been found to have a positive impact on patient satisfaction and may positively affect patient health behaviors and health outcomes. Such skills are also essential for accurate, succinct, and clear peer-to-peer (physician to-physician), physician-to-lay-public, and physician-to-media communications. These skills are not innate, however; they must be learned and practiced repeatedly. The Division of Medical Communications was created within the Department of Medicine at Brigham and Women's Hospital as an intellectual home for physicians who desire to learn and teach the wide variety of skills needed for effective communication

http://medicalcommunications.bwh.harvard.edu/ (accessed May 17, 2018). Thus, the mission of the Division of Medical Communications is to improve communication between physicians and patients, peers, the public and the media. *Id.* Gottesfeld points to no evidence that the availability or unavailability of any particular computer network at a separate hospital would have a material impact on Dr. Pfeffer's research and the mission of the Division of Medical Communications.

Gottesfeld speculates that the DDOS attack could have affected Dr. Pfeffer's non-financial interests in other ways that are even more attenuated. He argues: "[I]f Magistrate

Judge Bowler refused to issue the search warrant, information related to the alleged cyber attack may never have been learned, impairing the ability of HMS and BWH to learn about the attack and better prepare against future attacks. Granting the search warrant, however, increased the likelihood of acquiring such information." (Dkt. No. 166 at 8). The argument is entirely speculative, and in no way particularized to any interest of Dr. Pfeffer, financial or otherwise.

Gottesfeld's final effort is no better. He states:

> Similarly, if Magistrate Judge Bowler refused to issue the search warrant, the government may never have acquired evidence leading to Mr. Gottesfeld being charged (or convicted) with the DDOS attack; indeed, nobody had been charged in the approximately five (5) months between the April 2014 DDOS attack and the September 2014 application for the search warrant. Without criminal charges, HMS-affiliated hospitals would be deprived of the deterrent effect Mr. Gottesfeld's prosecution would have against future would-be hackers, creating more work for HMS affiliated hospitals in various respects, including but not limited to the field of medical communications."

The government agrees that there is general deterrent value in prosecuting individuals who attack hospital networks. But the affidavit did not address the impact of the DDOS attack on any specific hospital other than Children's Hospital, and Gottesfeld's speculation about how failing to prosecute him would "create[] more work for HMS and affiliated hospitals" was not a ground for recusal before the issuance of a search warrant. Gottesfeld's failure to cite a single case in support of his proposition is telling.

E. Judge Bowler's Recusal in *Cabi v. Boston Children's Hospital* is Inapposite.

At a May 3, 2018 hearing, the Court denied a then-pending motion to recuse Judge Bowler based on grounds similar to those addressed herein. Among other things, the Court found that Judge Bowler's recusal in *Cabi et al. v. Boston Children's Hospital et al.*, 15-cv-12306-DJC, provided no reason to believe that Judge Bowler should have recused herself from considering the warrant at issue in this case. In pressing his claim again, Defendant only

reinforces the Court's conclusion. *Cabi* involved an employment discrimination claim against Children's Hospital. Judge Bowler presided over the matter for approximately two years before an issue arose that *directly* implicated her husband's employer—a dispute over discovery of *HMS* documents regarding an internal investigation of allegations of research misconduct. Judge Bowler's decision to recuse herself at that point demonstrates both her awareness of her responsibilities to avoid even the appearance of impartiality, and her willingness to recuse herself out of an abundance of caution when she believes circumstances dictate. Consideration of the warrant presented no such circumstances, and she was correct to issue it.

F. There Was No Appearance of Bias.

Because Dr. Pfeffer's connections to HMS and BWH were so divorced from the attack on Boston Children's Hospital, no actual conflict existed that required Judge Bowler's recusal. *See supra*. Nor did these same attenuated ties, which Gottesfeld twists himself in logical knots to establish, create any appearance of bias in Judge Bowler. Disqualification is appropriate only where "the facts provide what an objective, knowledgeable member of the public would find to be a reasonable basis for doubting the judge's impartiality." *In re United States*, 666 F.2d 690, 695 (1st Cir. 1981). Recusal is "appropriate only when the charge is supported by a factual basis," *id.*, so that a judge should not recuse herself based on "misrepresentations or falsehoods," *id*. at 167 n.5.

Stripped of its misrepresentations, Gottesfeld's argument is that Dr. Pfeffer works at a medical school that has an academic affiliation with sixteen Boston area hospitals and research institutes, one of which—Children's Hospital—was a victim described in the government's search warrant affidavit. Despite his affiliation with the HMS, Dr. Pfeffer has no employment or accreditation relationship with Children's Hospital. Under these circumstances, no

knowledgeable member of the public would have a reasonable basis to doubt Judge Bowler's impartiality.

G. The Warrant Was Facially Valid.

Judge Bowler issued the warrant to search Gottesfeld's residence on September 29, 2014, at 3:43 p.m. (Dkt No. 78, Ex 2 (sealed)). The warrant identified the specific location to be searched on its face and did so again with greater particularity in Attachment A. *Id.* The warrant further identified the evidence to be seized on its face and did so again with particularity in Attachment B. *Id.* The incorporation of attachments with a warrant is proper, and Gottesfeld does not argue otherwise.

The warrant was supported by the affidavit of FBI Special Agent Michael Tunick. The affidavit established probable cause to search the location (described in Attachment A) and to seize evidence (described in Attachment B). (Dkt. No. 78, Ex. 2 (sealed)). The affidavit was "[s]ubscribed and sworn" before Judge Bowler on September 29, 2014. *Id.*

In his original motion to suppress, Gottesfeld alleged that the warrant lacked sufficient particularity with respect to the authorization to seize electronic devices. (Dkt. No. 78 at 16-17). The government responded to this issue in its original opposition. (Dkt. No. 84 at 21-23).

In his two supplemental motions, Gottesfeld alleges no other defect in the warrant itself. Instead, Gottesfeld notes that the cover page for the warrant application (Form AO 106) contains a typewritten date of September 30, 2014. (Dkt. No. 166 at 19). Magistrate Judge Bowler drew a line through the typewritten date, wrote September 29, 2014, and initialed the change.

The only reasonable conclusion to draw from these documents is that the application cover sheet contained a typographical error, stating 9/30/2014 instead of 9/29/2014. The handwritten dates and times on both the warrant and Special Agent Tunick's affidavit indicate they were signed on September 29, 2014, with the typographical error being on the cover sheet.

The government received copies of these documents containing the typo and produced them in discovery. Sometime after the documents were signed, but before they were docketed on September 30, 2014, Magistrate Judge Bowler became aware of the typo and corrected it by hand.

Rejecting reason, Gottesfeld asks this Court to conclude that "the 'Application for a Search Warrant' and accompanying affidavit of special agent Tunick was not submitted until *the day after*" the warrant was signed. (Dkt. No. 166 at 18). Perhaps realizing the absurdity of his claim, defendant contends that even if the warrant and application were executed on September 29, 2014, the typographical error on the cover sheet constitutes a defect in the "form of the warrant vis-à-vis its application" (Dkt. No. 166 at 19)—a newly minted theory without any support in the case law. To the contrary, the application and the warrant are distinct documents. *E.g.*, *Groh v. Ramirez*, 540 U.S. 551, 557–58 (2004) ("The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents"). A defect in the warrant cannot be cured by an unincorporated application, *id.*; likewise, a typographical defect in an application will not vitiate the legality of a facially valid warrant. *E.g.*, *United States v. Butler*, 594 F.3d 955, 961–62 (8th Cir. 2010) (typographical error involving date of controlled drug purchase did not cast doubt on probable cause). Indeed a typographical error involving a type-written date on the *warrant itself* does not necessarily vitiate the warrant. *See United States v. White*, 356 F.3d 865, 869 (8th Cir. 2004).

H. The Warrant's Supporting Affidavit Established Probable Cause.

Initially, Gottesfeld argued that the affidavit failed to establish probable cause only when IP and associated domain information was excised from the analysis. (Dkt. No. 78 at 15-16). He now claims that the affidavit fails to establish probable cause on its face. (Dkt Nos. 166 at 17; 128 at 15). The government has previously argued that the affidavit established probable

cause even without reference to information obtained from the PRTT and reincorporates that argument herein. The government addresses the issue further only to identify the appropriate standard for review and to respond briefly to Gottesfeld's new arguments.

Where, as here, a defendant challenges a magistrate judge's probable cause determination, the reviewing court should simply ensure that the magistrate judge had a substantial basis for concluding that probable cause existed. *See United States v. Feliz*, 182 F.3d 82, 86 (1st Cir. 1999); *United States v. Taylor*, 985 F.2d 3, 5 (1st Cir. 1993). "[A] magistrate's determination of probable cause should be paid great deference by reviewing courts." *Illinois v. Gates*, 462 U.S. 213, 236 (1983) (quotation omitted). Moreover, even in doubtful or marginal cases, reviewing courts still defer to an issuing magistrate judge's probable cause determination. *See United States v. Ventresca*, 380 U.S. 102, 107 (1965); *Rosencranz v. United States*, 356 F.3d 310, 316 (1st Cir. 1997) ("The Supreme Court made it perfectly clear that . . . doubtful cases should be resolved in favor of the warrant."). It is well-established that "[t]he standard of probable cause is the probability, not a *prima facie* showing, of criminal activity. Courts should not subject the affidavit to *de novo* review and should give 'great deference' to the magistrate's determination of probable cause." *United States v. Ciampa*, 793 F.2d 17, 22 (1st Cir. 1986) (citation omitted).

A search warrant application must meet two requirements. It must demonstrate probable cause to believe that: "(1) a crime has been committed (the commission element); and (2) particular evidence of the offense will be found at the place to be searched (the nexus element)." *United States v. Serrano*, 632 F. Supp. 2d 100, 105-106 (D. Mass. 2009) (citing *United States v. Ribeiro*, 397 F.3d 43, 48 (1st Cir. 2005)).

Special Agent Tunick's affidavit met both requirements. Gottesfeld quibbles with certain word choices, but his arguments do not undermine the existence of probable cause. For example, Gottesfeld suggests that Agent Tunick's statement that "the group Anonymous is known for numerous hacking attacks, many of which involve DDOS attacks," was not properly supported. Dkt. No. 128 at 16. However, the statement, made under oath, was based on Special Agent Tunick's "training and experience." That training and experience was summarized earlier in the affidavit and provides a sound foundation for the statement.

Defendant further alleges that Special Agent Tunick's mischaracterized a pastebin posting that included information regarding a Children's Hospital server. (Dkt No. 128 at 16). Specifically, he alleges that Special Agent Tunick omitted the fact that the pastebin post included publicly available information about Children's Hospital including its mailing address and website address, presumably to suggest that the post called only for lawful activity. *Id.* In fact, Special Agent Tunick did not omit this information at all. He described the pastebin posting in detail, listing the very information that Gottesfeld accuses him of omitting—including the hospital name, address, telephone number and website (along with the IP address and server type that were necessary to initiate the DDOS attack). (Dkt. No. 78, ¶ 13 (sealed)).

Gottesfeld also argues that his letter to Greatschools.org should not have been characterized as "threatening." (Dkt. 128 at 17). Special Agent Tunick's characterization was appropriate, however, and in any case, he provided the relevant substance of the letter, thereby allowing the Court to interpret the conduct for itself.[4] (Dkt. No. 78, Ex A (sealed) at ¶ 31).

[4] Gottesfeld also contends that it was misleading to state that the Commonwealth of Massachusetts took custody of a minor from her parents based on a "serious medical condition." This description, while relevant context, was not material evidence establishing probable cause. References to the YouTube video provided Gottesfeld's perspective on the matter for the Court's consideration.

Gottesfeld's argument that his YouTube video was protected speech, (Dkt. No. 128 at 17-18), and therefore cannot form the foundation for probable cause, goes nowhere. Posting the video was not the crime under investigation. Rather, the video was highly relevant to various crimes under investigation and was one piece of evidence among many establishing probable cause to believe that evidence of those crimes would be located in Gottesfeld's apartment. ¶

I. Gottesfeld Failed to Meet His Burden of Showing that Any Particular Piece of Evidence He Seeks to Suppress Is a "Fruit" of Port Data.

To prevail on a motion to suppress, "a defendant must establish a nexus between the Fourth Amendment violation and the evidence that he seeks to suppress." *United States v. Kornegay*, 410 F.3d 89, 93–94 (1st Cir. 2005) (citing *Alderman v. United States*, 394 U.S. 165, 183 (1969)). Only after a defendant meets this initial burden does the burden shift to the government to establish that the evidence "would have been inevitably discovered, was discovered through independent means, or was so attenuated from the illegality as to dissipate the taint of the unlawful conduct." *Kornegay*, 410 F.3d at 93 n.4.

Gottesfeld alleges that the collection of port data associated with his internet traffic violated his Fourth Amendment rights, but he establishes no nexus between the collection of port data and any evidence derived from its collection. *See id*. The search warrant affidavit makes not one reference to port data. This stands in contrast to the Gottesfeld's first motion to suppress, where he challenged the collection of IP data, and argued that the IP data, which was referenced in the affidavit, was essential to establishing probable cause to obtain the warrant. (Dkt. No. 78 at 15-18). The absence of any connection between the port data and the government obtaining the search warrant is fatal to his claim, and the Court should deny the motion as applied to port data on this ground alone.

To the extent the Court addresses the merits regarding the collection of port data, Gottesfeld's motion should be denied for the reasons described below.

J. Port Numbers are "Dialing, Routing, Addressing, or Signaling Information Within the Meaning of the Pen/Trap Act.

Gottesfeld acknowledges that the Pen/Trap Act authorizes the collection of "dialing, routing, addressing, or signaling information," but not "content." (Dkt. No. 128 at 4). As described in the government's response to Gottesfeld's original motion, when the Act was amended in 2001, Congress specified that it was intended to allow the collection of non-content addressing information for internet communications as well as more traditional forms of communication. (Dkt. No. 84 at 3).

A port number, as Gottesfeld describes, is the portion of an internet packet that "is used to direct the packet once it reaches the host computer at the destination IP address." (Dkt No. 128 at 6). The port number, in effect, tells the computer how to handle an incoming packet—what protocol it is using and how to process it.[5] Like an IP address, the purpose of a port number is to route Internet traffic to its proper destination. IP addresses achieve this by directing a packet to a particular computer, while port numbers direct a packet to a particular program within that computer. As noted in authority Gottesfeld cites, if an IP address is analogous to a physical address, "a port number more or less corresponds to a room in the building." Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, 30 HARV. J. L. & TECH. 1, 42 (2016) (cited at Dkt. No. 126 at 4, 5, 10, 11).

[5] Lydia Parziale et al., *TCP/IP Tutorial and Technical Overview*, IBM, at 144–45 (2006), available at http://www.redbooks.ibm.com/pubs/pdfs/redbooks/gg243376.pdf.

Port numbers are a portion of the TCP header,[6] which is frequently collected along with IP addresses with a Pen/Trap order. *See, e.g., United States v. Ulbricht*, 858 F.3d 71, 98 n.29 (2d Cir. 2017) ("The issue presented in this case is narrowly confined to orders that are limited to the capture of IP addresses, TCP connection data, and similar routing information.").

In its application for an order authorizing use of a PRTT device in this case, the government expressly stated that it did not seek "content," and it described the various types of non-content information that it did wish to collect. The application described port numbers, and the PRTT order specifically authorized their collection. (Dkt. No. 78, Ex. C at 2).

K. Port Numbers Are Not "Content."

Defendant contends that "[p]ort numbers . . . are *per se* the private contents of 'conversation,'" (Dkt. 128 at 11), but this claim is without merit. Information is content within the meaning of the Pen/Trap Act if it conveys the "substance, purport, or meaning" of a communication. 18 U.S.C. § 2510(8). Port numbers no more convey "substance, purport, or meaning" than do telephone numbers (the capture of which was the original purpose of pen registers) or IP addresses. *See Ulbricht*, 858 F.3d at 96 n.26 ("Like IP address data, the TCP data that the [PRTT] orders permitted the government to acquire do not include the contents of communications," and noting that defendant expressed no concern about the collection of port data as opposed to IP data).

Indeed port numbers usually convey much less than telephone numbers or IP addresses. Gottesfeld's own "sample profile," *see* Dkt. No. 128 at 7-8, demonstrates this fact. Defendant describes port numbers that would reveal that a user sent email, worked from home or remotely,

[6] TCP, or Transmission Control Protocol, is one of the main protocols used for Internet connections. It allows the creation of a stable connection between two computers across which data can be exchanged. Parziale, *supra* note 5, at 7–8. *See also*, *Ulbricht*, 858 F.3d at 95 n.6.

or visited websites. *Id.* He provides no example, however, of a port number that would reveal the content of an email that was sent or a site that was visited—because port numbers cannot reveal such information. For example, virtually all traffic to a website will use port 80 or 443, whether the site is a dating site, an employer's web site, or anything in between.[7]

Much of Gottesfeld's "sample profile" appears to be based on inferences drawn from IP data, not port data. *See* Dkt. No. 126 at 3-8. In any case, inferences drawn from port data are, if anything, less meaningful that those drawn from other types of non-content routing data. Addressing a PRTT for email communications, the Ninth Circuit explained:

> At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses—but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.

*United States v. Forrester*, 512 F.3d 500, 503 (9th Cir. 2008).[8]

---

[7] *See Service Name and Transport Protocol Port Number Registry*, Internet Assigned Numbers Authority, available at https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml (assigning port 80 to HTTP traffic and port 443 to HTTPS traffic).

[8] The government notes that a PRTT on an email account would not be possible at all under Gottesfeld's construction of the statute, as metadata concerning email communications necessarily reveal that the use of the internet to engage in email communications. By Gottesfeld's standard, this metadata would necessarily concern the "purport" of the communication and therefore constitute "content."

In any event, port numbers do not necessarily reveal the type of internet traffic to an outside observer, since it is possible to set up a connection between two computers to use a port other than the "assigned" one. Port assignments are essentially conventions, and they are not universally adhered to in practice. *See*, Silvio Valenti et al., *Reviewing Traffic Classification*, *in* DATA TRAFFIC MONITORING AND ANALYSIS 126 (Ernst Biersack, Christian Callegari & Maja Matijasevic eds., 2013) (describing port-based traffic analysis as "largely unreliable" because of applications using non-standard ports). As Gottesfeld's own authorities make clear: "**Ports Cannot Be Trusted[.]** It is important to remember that port assignments are standards, but they are not set in stone. Servers can be run on ports that are unassigned or are assigned to other protocols."[9] Dkt. 128, Ex. 2 at 5 (emphasis original).

Gottesfeld analogizes port numbers to "post-cut-through dialed digits" to suggest that both are content, (Dkt. 128 at 11), but he ignores the nuanced approach that courts have taken to post-cut-through digits. As the D.C. Circuit held in *U.S. Telecom Association v. FCC*, 227 F.3d 450 (D.C. Cir. 2000), some post-cut-through digits are content, and some are not. *Id.* at 462. For example, when an individual dials an extension or uses a calling card, they enter post-cut-through digits that are clearly only routing information. *Id.* If someone enters an account number, password, or the like into an automated system, that could qualify as content. *Id.* Some courts, concerned about the possibility of inadvertent collection of content, have refused to allow the collection of post-cut-through digits. *See In re Certified Question of Law*, 858 F.3d 591, 597–98 (FISA Ct. Rev. 2016) (collecting cases). There can be no analogous concern for port numbers, however. Port numbers always serve the same purpose, one analogous to a phone

[9] The (unidentified) author of Exhibit B to Dkt. No. 128 goes on to describe his ability to circumvent security protocols for a Department of Defense server by manipulating the port number assigned to particular types of internet traffic. *Id*. at 6.

extension; they instruct the destination computer to direct a packet to a particular program within the computer. They are fundamentally routing data, and therefore may be collected under the Pen/Trap Act.

L. Any Subjective Expectation of Privacy in Port Numbers Is Objectively Unreasonable.

Gottesfeld has filed an affidavit in which he states that he "operated with a reasonable expectation of privacy as to the Internet Protocol (IP) Addresses with which I was communicating as well as to the UDP and TCP port numbers on any Internet Protocol packets" at issue. (Dkt. No. 175, Ex. A).

Even if Gottesfeld has a subjective expectation of privacy, that expectation is not one that society recognizes as reasonable. As the government argued in its initial response in relation to IP addresses, routing information, including port numbers, is disclosed to ISPs in order to facilitate Internet communications. *See* Dkt. 84 at 11; *Ulbricht*, 858 F.3d at 97. Defendant's statement that "the information conveyed by a port number is not made available to any third party," is simply not accurate. Port numbers are transmitted in unencrypted form, even when an individual uses privacy-protective tools like Tor.[10] One of Gottesfeld's primary authorities cited in his brief expressly states that ISPs monitor port data for various reasons. 30 HARV. J. L. & TECH. AT 48-49 (describing ISP monitoring of port numbers).

Recognizing that routing information is disclosed, Congress has incorporated a routing/content distinction into the Pen/Trap Act—the same line drawn by the Supreme Court in *Smith*. See H.R. Rep. No. 107–236, at 53 (Oct. 11, 2011) (citing *Smith*, 442 U.S. at 741–43). The Supreme Court has not overturned or limited *Smith*, and unless and until it chooses to do so,

[10] *See* Tor Protocol, https://wiki.wireshark.org/Tor (describing how an observer can capture traffic using Tor software by filtering based on port numbers).

this Court is bound by its holding that there is no reasonable expectation of privacy in non-content routing information.

M. Law Enforcement Was Entitled To Rely on a Presumptively Constitutional Statute and a Duly Executed Order of the Court in Obtaining the Port Data at Issue.

The government previously argued with respect to obtaining IP data under the Pen/Trap Act that it was entitled to rely on a presumptively constitutional statute. Dkt. No. 84 at 17-19. Those arguments apply with equal force to the collection of port data obtained under the same statute. The government accordingly incorporates those arguments herein by reference. As was the case with IP data, available precedent supports the government's position that port data is non-content "dialing, signaling, addressing, or routing" information within Pen/Trap Act. *See Ulbricht*, 858 F.3d at 96 n.26. Under such circumstances, "an officer cannot be expected to question the judgment of the legislature that passed the law" and therefore suppression "cannot logically contribute to the deterrence of Fourth Amendment violations." *Illinois v. Krull*, 480 U.S. 340, 349-50 (1987). *Cf. Davis v. United States*, 564 U.S. 229, 241 (2011) ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule"). *See also United States v. Russell Rose*, 914 F. Supp. 2d 15, 22-24 (D. Mass. 2012) (Gorton, J.) (applying *Davis* to deny motion to suppress warrantless GPS tracking evidence where officers reasonably relied on non-binding precedent). Such reliance is all the more reasonable when law enforcement sought and obtained a court order from a neutral magistrate, Magistrate Judge Jennifer C. Boal. Under such circumstances, suppression would serve no Constitutional interest.

N. Law Enforcement Relied in Good Faith on a Facially Valid Warrant.

As stated in the government's previous opposition, even if this Court deemed the warrant deficient, "it could hardly be called so overbroad (or lacking in probable cause) 'as to render

official belief in its [validity] entirely unreasonable.'" *United States v. Jenkins*, 680 F.3d 101, 107 (1st Cir. 2012) (quoting *Leon*, 468 U.S. at 923). This is a far cry from the rare case where a warrant is so clearly insufficient as to merit the "extreme sanction of exclusion[.]" *Leon*, 486 U.S. at 926. *Cf. United States v. Ricciardelli*, 998 F.2d 8, 15 (1st Cir. 1993) (exclusion not proper where existence of probable cause was a "borderline call"); *United States v. Beckett*, 321 F.3d 26, 32-33 (1st Cir. 2003) (exclusion not proper even when evidence of nexus between criminal activity and residence was "less than overwhelming"). Because it cannot "be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment," *Leon*, 468 U.S. at 919, applying the exclusionary rule would not deter future Fourth Amendment violations and therefore is inappropriate in these circumstances, *Krull*, 480 U.S. at 347.

Gottesfeld attempts to circumvent this principle by arguing that Judge Bowler was not serving as a "neutral and detached" judicial officer. For the reasons described above, this is simply untrue. But even if there were an actual conflict of interest rising to the level of a constitutional violation, there is no suggestion that Special Agent Tunick, who obtained the warrant, was aware of it. Suppression would therefore do nothing to deter police misconduct, which is the sole purpose of the exclusionary rule. *See United States v. Leon*, 468 U.S. 897, 906, 916 (1984) (exclusionary rule is a "judicially created remedy" that is "designed to deter police misconduct rather than to punish the errors of judges and magistrates.").[11]

[11] *See generally* 2 Wayne R. LaFave, Search & Seizure § 4.2 (5th Ed. 2017 Update) ("[I]t would seem . . . that whether the person who issued the warrant in fact qualified as a neutral and detached magistrate is no longer determinative on the suppression issue. Rather, the question is whether it was "objectively reasonable" for the officers who obtained and executed the search warrant to assume that the person issuing it was constitutionally authorized to do so. As is highlighted by the fact that the Court in Leon concluded the exclusionary rule was unnecessary to deter magistrates from engaging in improper conduct, this means that neither intense bias by

For all of these reasons, the Court should deny Gottesfeld's Motion to Suppress.

Respectfully submitted,

Andrew E. Lelling
United States Attorney

By: */s/ David J. D'Addio*
David J. D'Addio
Seth B. Kosto
Assistant U.S. Attorneys

the issuing magistrate nor his total failure to assess the search warrant affidavit requires suppression unless the police reasonably should have known the facts demonstrating those circumstances.")

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

*/s/ David J.D'Addio*

Dated: May 18, 2018